ABSTRACT OF THE DISCLOSURE

A signature device 2 creates encrypted data by encrypting a first element of a member certificate through use of a first random number and public information disclosed by said group management device 1. The signature device 2 also creates first and second converted data by converting the first element through use of a random number and public information. The signature device 2 further creates knowledge signature data from which information concerning the first element, the second element, and the signature key will not be divulged, and outputs a group signature which contains the knowledge signature data together with a message. A verification device 3 verifies whether a group signature has been created by using a member certificate of one of the registered members in the group and a signature key, based on the message, the group signature, and the public information.